BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

In the Matter of:	
Protecting the Privacy of Customers of Broadband and Other Telecommunications Services	WC Docket No. 16-106
In the Matter of	
Lifeline and Link Up Reform and Modernization, Telecommunications Carriers Eligible for Universal Service Support, Connect America Fund	WC Docket Nos. 11–42, 09–197, and 10–90

COMMENTS OF THE GREENLINING INSTITUTE AND MEDIA ALLIANCE ON PROTECTING THE PRIVACY OF BROADBAND AND OTHER TELECOMMUNICATIONS CUSTOMERS

Paul Goodman
Senior Legal Counsel
The Greenlining Institute
1918 University Avenue, 2nd Floor
Berkeley, CA 94704
(510) 926-4000
paulg@greenlining.org

Tracy Rosenberg
Executive Director
Media Alliance
2830 20th Street, Suite 102
San Francisco CA 94110
(415) 746-9475
Email: tracy@media-alliance.org

TABLE OF CONTENTS

I. INTRODUCTION

The Greenlining Institute (Greenlining)[1] and Media Alliance[2] (sometimes California Groups or California Consumer Groups) submit these comments in response to the Notice of Proposed Rulemaking (NPRM) adopted by the Federal Communications Commission (FCC or Commission) on March 31, 2016, and released on April 1, 2016, related to the privacy of broadband and other telecommunications customers,[3] and in response to CTIA's Petition for Partial Reconsideration in the Lifeline proceeding.[4] Both the NPRM and the CTIA Petition raise profound questions of what privacy means when our lives are lived online, when our personal information – gleaned from our interaction with the transport network –becomes a commodity, and when the harvesting of our personal information often occurs with little or no awareness of it by us, the persons whose data it is.[5]

The California Consumer Groups applaud the FCC for its timely (and courageous) step of putting the privacy question on the agenda in this expanded context, and embrace the FCC's objectives of extending "transparency, choice, and data security" to broadband

[1] The Greenlining Institute represents a coalition of low-income and minority groups in state and federal proceedings. Greenlining believes that communities of color and people of all income levels should have access to a reliable and trustworthy broadband infrastructure. *See* www.greenlining.org

[2] Media Alliance was formed in 1976 with the belief that in order to ensure the free and unfettered flow of information and ideas necessary to maintain a truly democratic society, media must be accessible, accountable, decentralized, representative of society's diversity, and free from covert or overt government control and corporate dominance. *See* www.media-alliance.org.

[3] *In re Protecting the Privacy of Customers of Broadband and other Telecommunications Services,* Notice of Proposed Rulemaking, FCC Release 16-39, in WC Docket 16-106 (April 1, 2016) (*Broadband Privacy NPRM*).

[4] CTIA Petition for Partial Reconsideration, *In re Lifeline Reform and Modernization,* WC Docket 11-42 et al. (Aug. 13, 2015).

[5] NPRM, at ¶ 3.

services.[6] Some consumers are willing to trade their data for services rendered. Many, however, have no idea how far their data travels, how it is commoditized, and to what purposes it is put. If anything, the *Broadband Privacy NPRM* does not go far enough in coming to terms with this rapid development. Greenlining and Media Alliance urge the Commission to adopt bright-line and enforceable privacy protections that apply to all segments of the telecommunications world – voice, BIAS, and wireless. The California Groups focus these Comments on the following points:

> (1) the Commission should consider the dangers to consumers inherent in the close relationship between broadband telecommunications providers on the one hand, and data marketers on the other hand;
>
> (2) the relationship between telecommunications carriers and data marketers has in effect created a two-sided market, in which the broadband Internet access service (BIAS) provider sells broadband to the consumer, and consumer information to the data aggregator or marketer;[7]
>
> (3) the conceptual key to protecting broadband consumers' privacy is to separate the transport function, the transmission by wire or radio, from the payload, the content and services available online. Separating, in other words, the telecommunications and information markets. Giving consumers as much choice as possible about how their data will be used, and separating those choices from consumers' choice of telecommunications services, is consistent with the FCC's *Open Internet*

---

[6] *Broadband Privacy NPRM*, at ¶2.

[7] This is (at least) a two-sided market separate and distinct from the two-sided market often glimpsed in the Comcast-Netflix dispute. *See Open Internet Order*, *infra*, at ¶¶ 338, 364; *compare* "The economic value of personal data for online platforms, firms and consumers," *http://bruegel.org/2016/01/the-economic-value-of-personal-data-for-online-platforms-firms-and-consumers/* ("two-sided market mechanism … online platforms act as intermediaries to collect data from consumers and sell advertising slots to companies"); *see also* Report of the U.K. Competition and Market Authority, "The Commercial Use of Consumer Data," at 9, 78, *passim* (viewing both data and privacy as markets), available at *https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf;* World Economic Forum, "Big Data, privacy and the huge opportunity in the monetization of trust" (same), available at *https://www.weforum.org/agenda/2012/01/davos-daily-big-data-privacy-and-the-huge-opportunity-in-the-monetization-of-trust.*

Order, which also separated the telecommunications and information markets, and allowed consumers to make separate choices about each;

(4) the Commission should include directory listing information within the full ambit of privacy protection, as most broadband is bundled with voice service, giving carriers the opportunity to sell their directory listing databases. These consist of the subscriber's name, address and telephone number - key building blocks in a data marketer's customer profile. The need for this protection is all the more acute because the directory listing function has been turned over to the marketplace, allowing any "directory provider" or "directory assistance service" to obtain the carrier's database on equal terms with every other.[8] Once so packaged, the data can easily migrate from the directory listing world to the data marketing world;

(5) the Commission should *deny* the CTIA Petition to reduce consumer protections for low-income telecommunications customers; and

(6) the Commission should undertake the difficult task of ensuring that consumers receive meaningful disclosure about how their personal information might be used, how far it might travel, and who might have access to it – current marketplace disclosures are confusing, at best.

These comments are framed by our awareness that information has become a commodity, where:

> Every keystroke, each mouse click, every touch of the screen, card swipe, Google search, Amazon purchase, Instagram, "like," tweet, scan – in short, everything we do in our new digital age can be recorded, stored, and monitored.[9]

Although most businesses in the Internet space, from Facebook to Google to Apple, are engaged in in some way in the information marketplace, the telecommunications carriers addressed in this inquiry occupy a special place and have the broadest view of their end-users' activities, as they control the physical layer of

[8] 47 USC 251(b)(3) ("nondiscriminatory access to … directory listing[s]"). This has spawned litigation between would be directory listing agencies, directory assistance providers, and carriers, concerning the terms and conditions of those sales, as described below.

[9] David Harcourt, *Exposed, Desire And Disobedience In The Digital Age*, at 1 (2015, Harvard U. Press).

transmission between the end-user and information and services at the network's edge. As a result, broadband telecommunications carriers can collect all the telemetry of those transmissions, and mate them with the end-user's directory and subscription information. This is true for both wireline and wireless communications.

The extent of consumer data harvesting by telecommunications carriers and their business partners is an underreported and not clearly understood phenomenon, despite reports by the Federal Trade Commission, the Government Accounting Office, and the Senate Commerce Committee, at least partly because the data marketing industry operates behind a "veil of secrecy."[10] People may be generally aware that they are, in some sense, trading their personal information for access to online services and content, but the specifics of this "trade" are startling, and call into question whether consumers actually understand the deal they have struck. In a response to a lawsuit filed by a German parliamentarian requesting all data collected on him by his wireless provider, the carrier – after months of delay and appeals – produced 35,830 lines of code, a detailed, a nearly minute-by-minute account of half a year of his life, including where he had travelled, whom he had contacted and from where, and (presumably) what Internet searches and transactions he had made along the way.[11]

---

[10] Senate Committee on Commerce, Science and Transportation, "A Review of the Data Broker Industry: Collection Use and Sale of Consumer Data for Marketing Purposes" (December 2013), at iii. available at http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=bd5dad8b-a9e8-4fe9-a2a7-b17f4798ee5a (reporting the "secretive" attitude of data brokers when asked about the sources of their data). *See* further discussion below.

[11] German politician Falke Spitz describes his experience in a TED talk. *See* http://www.ted.com/talks/malte_spitz_your_phone_company_is_watching.

The dangers of such data harvesting are increasingly evident, and they can start with something as apparently harmless as a telephone number, which in fact is a key organizing element in consumer data profiles. Charles Guthrie, an elderly veteran, was bilked of his life savings after he used his telephone number to enter a sweepstakes drawing, which caused his name and phone number to appear on a marketing list. The list was then sold by commercial data broker InfoUSA to a group of thieves, who used the information to defraud him:

> InfoUSA advertised lists of 'Elderly Opportunity Seekers,' 3.3 million older people 'looking for ways to make money,' and 'Suffering Seniors,' 4.7 million people with cancer or Alzheimer's disease. 'Oldies but Goodies' contained 500,000 gamblers over 55 years old, for 8.5 cents apiece. One list said: 'These people are gullible. They want to believe that their luck can change.' As Mr. Guthrie sat home alone -- surrounded by his Purple Heart medal, photos of eight children and mementos of a wife who was buried nine years earlier -- the telephone rang day and night.[12]

Other available information about Mr. Guthrie was likely appended to his telephone number, categorizing him as a vulnerable senior citizen. The phone was the medium that allowed repeated data broker sales of that information, and repeated fraudulent contact of an at risk person. In the Comcast case described below, victims whose name, address, and telephone number had been inadvertently released onto the Internet reported an immediate and sharp spike in telemarketing calls.[13] When the

---

[12] Charles Duhigg, Bilking the Elderly with a Corporate Assist, New York Times, May 20, 2007. http://www.nytimes.com/2007/05/20/business/20tele.html?_r=1 (visited May 1, 2016); *see also* Duhigg,

[13] Staff Opening Brief, *infra*, at 5-6; Reply Brief, *infra*, at 59 (citing underlying evidence).

directory or billing information of a voice customer is combined with the vastly larger pool of data available to a broadband provider, the dangers are exponentially worse.

It is important that the FCC grasp the problem both in its widest dimensions and on the basis of specific privacy abuses. Commenting Parties are from California, and address these Comments to a digital future created in part only a short freeway ride from our offices. This future is both promising and foreboding. It has global dimensions and ramifications. Technologists and policy makers around the world have begun referring to "the California challenge."[14] Reflecting the local/global nature of the problem, a recent privacy enforcement action of the California Public Utilities Commission (CPUC), concerning a data breach that affected thousands of Californians and others across the country, speaks to many of the questions posed in the *NPRM* as well as privacy issues debated worldwide.

II. THE CALIFORNIA DATA BREACH INVESTIGATION AND SETTLEMENT AGREEMENT, AND THE CONTINUITY OF PRIVACY ISSUES ACROSS PLATFORMS AND SERVICES.

In mid-2010, Comcast and its agents began inadvertently posting the names, addresses, and telephone numbers, of approximately 75,000 California customers (and thousands more across the country) *who had requested and paid for a non-published directory listing and/or unlisted telephone number*, on an Internet website, from which

[14] *See, e.g.*, online video report of conference in Germany under the rubric of "The California Challenge" ("*die kalifornische Herausforderung*"), at http://www.vernetzterleben.de/#information (in German and some English). English presentations by Aral Balkan on "Digital Emancipation: Ownership of the Self in the Digital Age," and Richard Barbrook on "Californian Ideology 20.2," both at http://www.vernetzterleben.de/home/mediathek/ (scroll down).

they were ripped and copied and passed throughout the Internet ecosystem. Comcast did not discover that this had occurred until October, 2012.

On September 17, 2015, the California Public Utilities Commission adopted an all-party settlement in its *Investigation into the Operations, Practices, and Conduct of Comcast Phone of California, LLC (U-5698-C) and its Unauthorized Disclosure and Publication of Comcast Subscribers' Unlisted Names, Telephone Numbers, and Addresses* (*Comcast Investigation*). The Settlement Agreement, and all filings in the proceeding, are available online.[15]

Greenlining was a party/intervenor in the *Comcast Investigation*. The Settlement called for Comcast to pay a $25 million penalty, provide another $8.3 million in restitution to consumers whose personal information had been disclosed against their wishes, and to adopt disclosure and data security measures designed to protect customer privacy going forward.

[15] The entire docket and all publicly filed documents are available online, at https://apps.cpuc.ca.gov/apex/f?p=401:57:0::NO (alternatively, go to http://delaps1.cpuc.ca.gov/CPUCProceedingLookup/f?p=401:1:32850522477459 and enter proceeding number I.13-10-003 without hyphens and with an "I" as in "Investigation" (I1310003); click on the Proceeding Number on the next page, and all filings ("documents"), rulings, and decisions are available). Testimony was not filed. Important filings in the docket include the Order Instituting Investigation 13-10-003, at http://docs.cpuc.ca.gov/SearchRes.aspx?DocFormat=ALL&DocID=78432340 ; Decision 15-09-009 Adopting Settlement at http://docs.cpuc.ca.gov/SearchRes.aspx?DocFormat=ALL&DocID=154462396 and http://docs.cpuc.ca.gov/PublishedDocs/Published/G000/M154/K462/154462396.PDF. The position of the parties is set forth in the Opening Briefs of CPUC Staff (http://docs.cpuc.ca.gov/PublishedDocs/Efile/G000/M143/K307/143307060.PDF), Comcast's brief (http://docs.cpuc.ca.gov/SearchRes.aspx?DocFormat=ALL&DocID=143310511), and TURN/Greenlining (joint brief) (http://docs.cpuc.ca.gov/PublishedDocs/Efile/G000/M140/K014/140014740.PDF); *see also* Staff Reply Brief (http://docs.cpuc.ca.gov/PublishedDocs/Efile/G000/M143/K990/143990273.PDF). Greenlining and Media Alliance thank CPUC staff for their assistance in the preparation of these Comments.

This privacy breach, and the resulting investigation by the California Public Utilities Commission and the California Attorney General, revealed facts, relationships, and realities in the communications, data-gathering, and data-marketing industries which relate directly to a number of questions posed by the NPRM, including: "whether there are certain BIAS provider practices implicating privacy that our rules should prohibit, or to which we should apply heightened notice and choice requirements";[16] whether and how to "harmonize" the privacy protection across largely converged voice and broadband services;[17] what is an adequate "data security framework" to "protect the security, confidentiality, and integrity" of customer information;[18] what constitutes "meaningful notice" and – more importantly – meaningful customer choice;[19] and what is the role of the states going forward.[20]

Although this breach occurred with regard to t*elephone* subscriber information, many of the victims were also subscribers of Comcast's *broadband* and cable services, and many of the structures, processes, and mechanisms – subscriber and billing information systems, often managed by third party contractors, and apparently regularly used by third party aggregators to "true up" their databases – are common to both services. Indeed, the Comcast privacy disclosure cited in the *NPRM* (and at issue in the CPUC investigation) is labeled a Privacy Notice "for Cable Video, High-Speed Internet,

[16] NPRM at ¶ 256.

[17] *Id.* at ¶ 152-53,

[18] NPRM at pars 174-175, and generally at ¶¶ 167-232.

[19] *Id.* at ¶¶ 27, 82.

[20] *Id.* at ¶¶ 276-77.

Phone, and Home Security Services," reflecting the bundled and overlapping nature of the services Comcast markets.[21] What are directory listings for the phone service are billing information in the broadband context. What is labelled a broadband line also carries voice communications. Directory listing and billing information become key relational points[22] to which other data elements are "appended," which in turn allows the creation of extensive consumer profiles, often organizing thousands of data points into a commercially useful roadmap of an individual's needs, habits, and aspirations.[23]

The broadband operator sits at the font of all this information – not as an edge provider like Facebook or Google, but as a provider of the network itself, in a position to capture every keystroke entered and website visited over the network connection. Directory and billing information and CPNI[24] may be combined with "unique device identifiers, IP addresses, persistent online identifiers (e.g., unique cookies), eponymous and non-eponymous online identities, account numbers and other account information, including account login information, Internet browsing history, traffic statistics,

---

[21] NPRM, at fn. 244, citing http://www.xfinity.com/Corporate/Customers/Policies/CustomerPrivacy.html (last visited May 21, 2016). The carriers' ability to change their websites and online disclosures from day to day presents an enforcement and challenge, and may warrant a requirement that the carriers maintain an archive of all past web disclosures.

[22] Telephone data, in itself, provides a treasure trove of data, as explained in Falke Spitz's TED Talk, *supra*. *See also* Schneier, *Data and Goliath* (2015), at 21 ("Telephone metadata alone reveals a lot about us. The timing, length and frequency of our conversations reveal our relationships with others: our intimate friends, business associates, and everyone in-between").

[23] *See, e.g.*, LaFond, "Third-Party Data: Are You Asking the Right Questions?" (March 24, 2015) ("Offline profile data providers have access to 1,000s of data points per profile and can find all the attributes your best customers have in common," compared to "an anonymous cookie [that] gathers data about where the visitor is spending time online as well as geographic details, [but] has fewer than 50 different pieces of targeting data available"), available at http://www.tru-signal.com/articles/data-audiences/third-party-data-are-you-asking-the-right-questions/ (last visited May 15, 2016).

[24] Customer Proprietary Network Information, defined at 47 USC § 222(c).

application usage data; current or historical geo-location, financial information (e.g., account numbers, credit or debit card numbers, credit history), shopping records, medical and health information, the fact of a disability and any additional information about a customer's disability biometric information, education information, employment information, information relating to family members, race, religion, sexual identity or orientation, other demographic information, and information identifying personally owned property (e.g., license plates, device serial numbers)," as well as other subscriber personal information like social security number and data and location of birth – and all this data is potentially available to the broadband provider.[25]

The "Stipulated Facts" incorporated in the Settlement Agreement explain how the data breach happened:

> (7) For varying periods of time between July 2010 to December 2012, and for many customers the entire period, approximately 75,000 Comcast residential subscribers in California who had paid Comcast the monthly fee for a non-published or non-listed phone number nevertheless had their subscriber listing information published on Ecolisting, and (in some cases) in phone books, and/or made available by a directory assistance provider. (See para. 9).
>
> (8) Comcast used a non-affiliated third party, Targus Info Services, Inc., later acquired by Neustar, to license its directory listings to various publishers and directory assistance providers, which Comcast does in the context of FCC rules.
>
> (9) Comcast has explained that, in connection with a system-wide account number change in California that occurred in October and December 2009, a significant portion of those California customers who elected non-published

[25] NPRM, at ¶ 62.

> status prior to December 2009 were mistakenly not flagged as "non-published" and thus were made available for publishing in July 2010 via Neustar. Comcast refers to this event as the "Process Error."
>
> (10) Until October 2012, it was Comcast's practice to send non-published listings to Neustar as well as published listings, while placing a "privacy flag" on the non-published listings. Because the "privacy flag" was not attached to the listings of approximately 75,000 non-published/non-listed subscribers, Neustar provided those listings to Comcast's vendor, Microsoft FAST, who then published them for Comcast on the Ecolisting website…
>
> (12) Neustar also provided the non-published subscriber listings to one nationwide directory assistance provider, kgb. kgb has been Comcast's directory assistance provider since at least 2009. Comcast believes that its contract with kgb effectively prohibits kgb from further sublicensing Comcast's listings…
>
> (14) Neustar erroneously provided a subset of the non-published/non-listed listings to one telemarketing company for testing purposes: Relevate. Relevate represented to Neustar that these non-published/non-listed listings were never used.

A further fact, stated in Comcast's Privacy Notice, is that once posted in an Internet directory, the data can be "sorted, packaged, repackaged and made available again in different formats by anyone."[26]

Commission staff and Greenlining contended that the breach occurred in part because of Comcast's decision to let a large data marketer act as a directory listing agent for Comcast, and the further decision to send even non-published/unlisted names,

[26] This language is in Comcast's Privacy Notice, both as litigated at the CPUC and as cited in the NPRM. *See* NPRM, fns. 183 and 244, and http://www.xfinity.com/Corporate/Customers/Policies/CustomerPrivacy.html.

addresses and telephone numbers to this agent.[27] The CPUC Investigation shed light on just how vulnerable personally identifying customer information is to disclosure, *even when all parties intend that it remain private*. Once the data was breached, the information can be sold and re-sold, travelling far and fast in the process.

III. PRIVACY PROTECTION DEPENDS ON SEPARATING THE TELECOMMUNICATION PROVIDER'S TRANSPORT FUNCTION FROM AFFILIATED DATA AND CONTENT MARKETS, WHICH IS CONSISTENT WITH COMMON CARRIAGE AND THE FCC'S *OPEN INTERNET ORDER*.

Perhaps the most important question the Commission asks is whether it should "prohibit the offering of broadband services contingent on the waiver of privacy rights by consumers."[28] There is nothing wrong with a consumer, after being fully informed, choosing to trade access to his or her personal data in return for enhanced services.[29] This becomes more problematic, although we do not exclude it categorically, when the choice is presented in the context of underlying network transport. Some consumers may want to purchase just the transport, i.e., stand-alone broadband transmission and Internet access with no ancillary services. Consumers should have this choice, and it should be as clear a choice as possible.

---

[27] *See generally* Staff Opening Brief, *supra*, at 7-10, 29-40.

[28] *Id.* at ¶ 256.

[29] Many of us have children and/or younger friends, from whom we hear that "privacy is no big deal." Our entirely unscientific study reveals that these same young adults, however, are often surprised to hear that their data is not used just by their wireless provider or by Google or other edge providers with whom they deal directly, but that it may become a commodity bought and sold throughout the data marketing industry.

The separation of conduit and content has been applied not only to telecommunications but other network industries.[30] Open networks are seen as a means to increase efficiency and eliminate conflicts of interest.[31] The principle of separation can remain a guiding principle as we watch what was formerly a telephone network become an all-purpose content distribution network, with former telephone companies buying up and integrating content and advertising affiliates into their transmission business, and former cable content providers moving into the business of broadband transport.[32] This mingling of conduit and content has not only increased the inherent

---

[30] Common carriage evolved in the railroad industry (certainly in California), and has also been applied (in different guises) to electricity (distributed generation), natural gas (generation unbundled from transmission), and telecommunications. *See* Reiter, "The Contrasting Policies of the FCC and FERC Regarding the Importance of Open Transmission Networks in Downstream Competitive Markets," 57 Fed. Comm. Law Journal 253 (2000).

[31] *Id.* at 253 ("pipelines were required to offer their open-access transportation services without discrimination or preference"), 304 (monopoly's "incentive to invest inefficiently - in closed proprietary networks"), 316 (goal of separation of communication from data processing was to "prevent carriers from discriminating in favor of their own information services over those offered by competitors by denying them access to needed telecommunications facilities")

[32] This evolution of course happened differently for telephone companies than it did for cable companies, but the end result are for both industries is that the transport and the content business is now vertically integrated. AT&T has merged with DIRECTV, and owns rights to or a stake in NFL Sunday Ticket, ROOT SPORTS, The Tennis Channel, MLB Network, NHL Network, and GSN (Game Show Network). *See* AT&T Completes Acquisition of DirectTV, at http://about.att.com/story/att_completes_acquisition_of_directv.html (visited April 28, 2016) (also noting AT&T's joint venture with Otter Media and its stake in Fullscreen—both apparent content-related relationships). Verizon acquired AOL last year, and recently acquired a stake in Awesomeness TV. *See* "Verizon Buys a Stake in Awesomeness TV …", at http://techcrunch.com/2016/04/06/verizon-buys-a-stake-in-awesomenesstv-to-bring-exclusive-videos-to-its-streaming-service-go90/ (visited March 28, 2016). The AOL acquisition also includes stakes in content providers like the Huffington Post, Engadget, and Techcrunch. *See* "Verizon to buy AOL for $4.4bn" at http://www.bbc.com/news/business-32702558 (visited April 29, 2016).

An outgrowth of this in California (and at the FCC) is the participation of new, content-focused parties like the Writers Guild of America West (WGAW) in cable and telecom merger proceedings, as well as the CPUC's ongoing *Telecommunications Competition OII*, CPUC docket sheet at https://apps.cpuc.ca.gov/apex/f?p=401:56:0::NO:RP,57,RIR:P5_PROCEEDING_SELECT:I1511007. In that proceeding, WGAW states that it is interested in "an open and competitive distribution market" for content produced by its members. April 19, 2016 WGAW Reply, at 3. Comcast objects to WGAW's

conflict of interest when one a carrier sells both transport and competing content, but exponentially increases the privacy exposure of consumers.[33]

The Commission notes that this *Broadband Privacy NPRM* was precipitated by the Commission's decision in the *Open Internet Order* to apply the existing (Section 222) privacy rules applicable to telecommunications carriers.[34] In referring to the *Open Internet Order,* the Commission acknowledges the importance of that Order's technology-neutral approach, treating all forms of telecommunication – landline telephony, broadband transmission, and wireless voice and data services -- under one regulatory framework, and tacitly answers its own repeated questions about whether the FCC should adopt a uniform set of rules for all telecommunications carriers.[35] Commenters believe that a uniform regime is not only easier for the carriers, easier of enforcement, and easier for customers to understand, it is also consistent with the *Open Internet Order* in terms of law and policy.

Open Internet rules are, at their core, anti-discrimination rules. This is the hallmark of "common carriage" as it has existed on the telephone network from the

---

access to confidential information on the ground that WGAW is a labor union involved in negotiations with some of Comcast's content affiliates. Comcast lists some of its content-related affiliates that negotiate directly with WGAW, including National Broadcasting Company, Universal City Studios, and E! Network Productions, LLC.

[33] *See, e.g.*, Comcast privacy notice, discussed *infra*, and its discussion of "activity data" ("information about the use of set top boxes, remote controls, electronic program guides, video players, applications, and other devices and software connected to our cable system. This information includes which channels, programs, and advertisements are viewed and for how long").

[34] *Id.* ¶13, citing *Protecting and Promoting the Open Internet, Report and Order on Remand, Declaratory Ruling, and Order,* 30 FCC Rcd 5601, 5791-98 (*Open Internet Order*), at ¶ 462.

[35] *See,.e.g., NPRM* at ¶ 166 (whether to "apply our proposed rules for BIAS providers' use and disclosure of, and access to[aggregate CPNI] to all other telecommunications carriers"); ¶ 81 (whether to apply rules to wireless carriers).

Kingsbury Commitments in 1913 through the 1934 Communications Act right up to 2002. In *Verizon v. FCC*, the D.C. Circuit traced the history of this concept:

> Although the nature and scope of the duties imposed on common carriers have evolved over the last century, the core of the common law concept of common carriage has remained intact … [with] the basic characteristic that distinguishes common carriers from "private" carriers--i.e., entities that are not common carriers--as "[t]he common law requirement of holding oneself out to serve the public *indiscriminately*."[36]

Non-discrimination inherently means separation of the transport function of telecommunications. The D.C. Circuit noted that the common carrier consensus came to an end with the FCC's 2002 *Cable Modem* (or *Cable Broadband*) decision that found broadband transport and information services were *not* separable,[37] and that this was the primary problem in applying the telecommunication law's long-standing prohibition of

[36] *Verizon v. FCC*, 740 F3d 623, 651 (DC Cir. 2014).

[37] *Id.* at 631:

> [In 2002], the Commission took a different approach when determining how to regulate broadband service provided by cable companies. *Instead of viewing cable broadband providers' transmission and processing of information as distinct services*, the Commission determined that cable broadband providers--even those that own and operate the underlying last-mile transmission facilities--*provide a "single, integrated information service.*" Because cable broadband providers were thus not telecommunications carriers at all, they were entirely exempt from Title II regulation.

(Emphasis added.)

discrimination to broadband.[38] The solution was to again separate telecommunications transport again, which the Commission did in 2015.[39]

When the principle of separation is forgotten, edge provider content and consumer information both tempt the carrier with the prospect of extra revenue from two-sided (or three-sided) markets. With content, the carrier can charge the consumer for broadband transport services, and charge edge providers for access to the consumer. With information, the carrier can charge the consumer for broadband transport services, and charge data marketers for access to the consumers' information.

A clear common carrier framework addresses both these problems. The *Open Internet Order's* "general conduct" rule – "no unreasonable interference or unreasonable disadvantage" standard[40] – echoes the FCC's finding in the instant *NPRM* that "practices that fail to protect the confidentiality of end users' proprietary information, will be unlawful if they unreasonably interfere with or disadvantage *end user's ability to select, access, or use broadband services*, applications or content."[41] Both discrimination in the carriage of edge-provider or subscriber-generated content, *and* the commodification and use of the consumer's personal information without informed consent, interfere with a

---

[38] *Id.* at 650:

> Given the Commission's still-binding decision to classify broadband providers not as providers of [separable] "telecommunications services" but instead as providers of "information services," *see supra* at 9-10, such treatment would run afoul of *section 153(51)*:"A telecommunications carrier shall be treated as a common carrier under this [Act] only to the extent that it is engaged in providing telecommunications services."

[39] *Open Internet Order* at ¶ 47 (BIAS "best viewed as separately identifiable offers of (1) a broadband Internet access service [BIAS] … and (2) various add-on applications, content, and services").

[40] *Id.* at ¶¶ 20-22 ("gatekeeper power can be exercised through a variety of technical and economic means").

[41] *NPRM*, at par 305, quoting from *Open Internet Order* at par 141 (emphasis added).

consumer's access to the BIAS telecommunications transport, and lessen consumer trust (and the public's trust) in the integrity of BIAS service. This violates in a real sense section 706 by discouraging "the deployment … of advanced telecommunications ability to all Americans,"[42] which in turn disrupts the "virtuous cycle" that has attended the explosive and reciprocal growth of the Internet and its underlying telecommunications substrate. Such was, of course, the logic of the *Open Internet Order*, and the Commission rightly concludes it should be the logic here. [43]

The separation between conduit and content is implicit in the statutory definition of telecommunications: "the *transmission*, between or among points specified by the user, *of information of the user's choosing, without change in the form or content* of the information as sent and received."[44] The separate and fungible provision of transport facilitates the customer's agency – the intended end-state of both non-discrimination and privacy rules.[45]

Privacy and non-discrimination are two sides of the common carriage coin, and have been at the core of the FCC's telecommunications regulation since its inception.[46]

---

[42] 47 USC § 1302(a).

[43] *NPRM* at par 309 (FCC belief that "the proposed transparency, choice, and security requirements further align with the virtuous cycle of Section 706, since they have the potential to increase customer confidence in BIAS providers' practices, thereby boosting confidence in and therefore use of broadband services, which encourages the deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans").

[44] 47 U.S.C. 153(50) (emphasis added).

[45] *See, e.g.,* NPRM at ¶ 309; *Open Internet Order* at ¶ 139 ("End-User Control").

[46] *See* 47 U.S.C. § § 201, 202 (non-discrimination); *compare* 47 U.S.C. § 705, discussed *infra***.**

With regard to the Communications Act's primary privacy protection, the Commission notes:

> Section 705 of the Communications Act has been in place since the adoption of the Communications Act in 1934. Section 705(a) establishes that providers of communications services by wire and radio have obligations not to "divulge or publish the existence, contents, substance, purport, effect, or meaning" of communications that they carry on behalf of others. We believe that Section 705 can thus provide a source of authority for rules protecting the privacy of customer information, including the content of their communications.[47]

Privacy, separation, and non-discrimination were non-controversial and taken for granted *until* the digital revolution, when the information carried on – and generated by - the network assumed an economic value independent of, and increasingly greater than, the value of the underlying communications services.[48] Common carriage persisted until 2002, and provided the framework for explosive growth of the Internet in the years leading up to 2002, and is doing so again today.

A clear concept of separation between conduit and content, between the business of communication transport and the business of data harvesting and sale, provides a framework for all of the issues discussed in the *NPRM*, including the dividing line between FCC and FTC jurisdiction, implicit in the FCC's discussion of the FTC's work.[49] Wired and wireless network transport is the FCC's domain; the information and

---

[47] *Broadband Privacy NPRM*, at ¶ 307.

[48] The DC Circuit notes that the FCC had treated advanced telecommunications services and Internet access as telecommunications services up to the *Cable Modem* decision in 2002. *Verizon v. FCC, supra,* 740 F.3d at 630-631 ("DSL services, the Commission concluded, involved pure transmission technologies").

[49] NPRM, at ¶¶ 8-9, 58, 71, 132, 237, 289, *passim.*

content services at the edge of the network are the FTC's bailiwick.[50] This division is not impermeable. There will be cases where the FCC will want, and should be able, to apply FTC fairness and reasonableness standards to telecommunications carriers.[51] And cases when a carrier's content affiliates may interfere or create a conflict of interest with the carrier's transport responsibilities. In the latter case particularly, a clear concept of telecommunications transport can provide decisive decisional guidance.

The understanding of communications transport as a separate, fungible service will also become important in judging the level of disclosure, customer awareness, and choice mechanism which is required before a carrier can offer "financial inducements, or less expensive or faster broadband, in exchange for the customer's "consent to use and share a customer's confidential information."[52] Protections are important to prevent "turning privacy from an essential human attribute to a market commodity," particularly for those people who value their privacy, or those without the means to secure premium privcy protection.[53] It will inform the Commission's decision to "prohibit the offering of broadband services contingent on the waiver of privacy rights by consumers," or – the more difficult task – require broadband carriers to offer a basic and affordable level of service without requiring the customer sacrifice his or her privacy to obtain it, as well as

[50] As the *Broadband Privacy NPRM* notes, the FTC is prohibited from regulating common carriers. pars 259, 306.

[51] *See NPRM* at ¶¶ 305-306, citing 47 USC 201 ("unjust and unreasonable" standard) and 202 ("unjust or unreasonable discrimination in charges, practices, classifications, regulations, facilities, or services").

[52] *Id.* at ¶ 259.

[53] *Exposed, Desire and Disobedience in the Digital Age, supra,* at 177.

persistent and recurring choice mechanisms allowing the consumer to tailor his or her privacy choices to an appropriate level.[54]

IV. WHAT THE COMCAST BREACH & SETTLEMENT TEACH US

There are any number of lessons that can be drawn from the Comcast data breach and its subsequent investigation and resolution, but the commenting parties wish to focus on three: (1) the relationship between the carrier and the data marketer, and the resulting temptation to monetize consumer data; (2) the difficulty in effecting adequate consumer disclosure and choice; and (3) the likelihood, even when consumers have made their privacy choices known, that profit-oriented companies will not invest adequate resources in protecting the consumers' personal information, absent a clear data security framework and stiff sanctions for non-compliance.

A. The Relationship Between Carrier and Data Marketer.

Commenting parties do not wish to single out Comcast or Neustar. We have no reason to believe their practices are appreciably better, different, or worse than other broadband providers and information aggregators or data marketers. They, however, present a case study of the symbiotic relationship between data transport and data marketing.

A second caveat is in order – there was no definitive evidence in the California record s to whether, and how much, Comcast may have profited by by working with Targus/Neustar. But circumstantial evidence, and repeated references in the privacy literature to a link between telephone numbers and other telecommunications utility data

[54] Apple phones, for example, allow the consumer to easily turn off the GPS mapping.

on the one hand, and data marketers on the other, support the inferences we draw from the evidence in *Comcast.*

While subscriber names, addresses and phone numbers – except for those of customers requesting non-published or unlisted status -- have traditionally been publicly available in printed phone books, a combination of digital technology, the deregulation of the telephone industry, and of directory services in particular in the 1996 Telecommunications Act, and the rise of "big data," have made directory listings a valuable commodity, and the source of numerous lawsuits.[55] The Federal Trade Commission (FTC), the Senate Committee, and the General Accounting Office (GAO) have all issued recent reports tracing the evolution and growth of the data broker industry, identifying (on less than complete data) telecommunications providers as one of the primary sources of such data.[56]

The FTC states that "Over half of the data brokers reported that they obtain other publicly available information, including telephone and other directories…."[57] The FTC refers to "data brokers that … obtain information from telephone companies about

[55] *See LSSi* litigation referenced below.

[56] Senate Committee on Commerce, Science and Transportation, "A Review of the Data Broker Industry: Collection Use and Sale of Consumer Data for Marketing Purposes" (December 2013), at iii. available at http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=bd5dad8b-a9e8-4fe9-a2a7-b17f4798ee5a (Senate Report); Federal Trade Commission, "Data Brokers – a Call for Transparency and Accountability"(May 2014), available at http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf (FTC Report); and US General Accounting Office (GAO), "Information Resellers – Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace" (September 2013), available at http://www.gao.gov/assets/660/658151.pdf (GAO Report).

[57] *See* FTC's "Data Brokers, A Call for Transparency and Accountability," *supra,* at 13.

consumers who have recently created a new landline account."[58] The GAO reports how large data brokers (Acxiom and Experian Marketing are the examples) combine "name, address, telephone number" with other demographic information such as education, occupation, party affiliation, ethnicity, marital status, household purchase behavior, household income, social media activity, hobbies, reading and music preferences, and ailments, *inter alia*, to create a consumer profile.[59]

The Senate Report describes how large utilities and other corporations can be both the source of data to, and purchasers of the completed data profiles from, the data resellers.[60] The utility's data is combined with other demographic information in a "data append" process:

> "Data append" products … require the data broker's client to provide some customer information, such as name and address; the client can then select additional information—such as the customers' telephone number and purchasing habits—that the data broker appends to the client's data set for the client's use in direct mail, telemarketing, and email marketing campaigns. Some products help clients fill in gaps that may exist in customer contact information. For example, the client may provide a customer's name and address, and the data broker could provide the customer's landline telephone number or email address. Alternatively, the client may provide the customer's landline telephone number, mobile telephone number, or email address, and the data broker could provide the customer's name and address …[61]

[58] FTC Report, at 14.

[59] GAO Report at Appendix II, "Examples of Data Collected and Used by Information Resellers."

[60] *See, e.g.*, Senate Report at 29 ("who buys the data … financial institutions, hotel chains, wireless telephone service providers, cable companies, and jewelry stores, as well as other data brokers or Resellers").

[61] FTC Report, at 24; *cf.* Schneier, *Data Goliath*, *supra*, at 41 ("Sometimes linking identities across data sets is easy; your cell phone is connected to your name, and so is your credit card").

The NPRM only fleetingly acknowledges the commercial value of the data at issue, and is largely silent on the role of data aggregators and marketers in the online ecology.[62] To the extent that online content is advertiser sponsored, consumer data is at a premium to enable targeted advertising and the nano-second negotiations for the placement of same. The CPUC proceeding suggests that there is significant pressure on telecommunications providers to either make their data available to data marketers, or to themselves monetize the data they have. CPUC staff argued that this pressure led to the provision by Comcast of both published and non-published account information to Targus/Neustar, and that Targus/Neustar then used this information to "corroborate" its own large consumer databases.[63] Comcast's practice put the personal and confidential customer information of non-published subscribers into the hands of data marketers, even if there were allegedly structural protections in place.[64]

Comcast worked with two large, well-known data brokers, Targus/Neustar and LSSi, to distribute and license its subscriber listings to third party directory publishers,

---

[62] *Compare* NPRM at¶ 263; *see also* footnote 222, citing letter from Twelve Public Interest Groups to Tom Wheeler, Chairman, FCC at 1-2 (Mar. 7, 2016), https://epic.org/privacy/consumer/Broadband-Privacy-Letter-to-FCC.pdf (noting Verizon, Comcast, and Cox all share targeting data with advertising-driven companies that they own, or with whom they are affiliated or partnered). Comcast alone has spent hundreds of millions of dollars in acquiring online advertising and data-targeting companies. *Id.* The Public Interest Groups further report that "Comcast is able to harvest 'terabytes of unstructured data' from the set-top boxes it controls, which it then enriches with demographic information to provide data 'more meaningful to advertisers,' including those targeted via 'Comcast's IP-based systems'."

[63] Staff Opening Brief *supra*, at ii, 9, 33, 35, 58, 107.

[64] The structural protections were allegedly limitations written into Comcast's contracts with LSSi and Targus/Neustar, limitations that may or may not have been observed in practice. *See* Staff Reply Brief, at 38.

assistance providers, and possibly others.[65] Comcast refers to Targus/Neustar as its "Listing Agent," but Targus and Neustar were much more. Neustar played a number of roles: (a) acting nationally as a NANC and number portability administrator; and (b) Neustar functioned in the Comcast case as a directory listing administrator, facilitating an open market in Comcast's directory listings (under the aegis, Comcast argued, of the 1996 Telecommunications Act).[66] and (c) operating as a data broker. A Comcast senior manager described Targus/Neustar as "a sophisticated data company … that focuses its business on managing and handling huge amounts of data."[67] Targus/Neustar officials refer to their company as "a commercial aggregator and provider of consumer and business data to third parties," including but not limited to directory listing publishers.[68] The Commission's expert witness Lee Tien bluntly described Targus/Neustar as a "data broker," an assertion Comcast did not challenge at the hearing.[69]

It was inevitable that Targus/Neustar's multiple, and (staff argued) conflicting, roles would meet, if not collide in the Comcast data breach, a breach for which Comcast

---

[65] *See, e.g.*, Staff Opening Brief at 7, *citing* Expert Testimony of Lee Tien at17-31, describing Targus/Neustar and LSSi as data brokers, and explaining what it is they do. As discussed below, Comcast claims that both companies were contractually prohibited from using the Comcast-provided directory listings for data marketing purposes, but Comcast admits it suspects that LSSi did not comply with this contractual provision, but asserts that Targus did comply.

[66] 47 USC § 251(b)(3); *compare* Comcast Opening Brief at 8 ("pro-competitive framework").

[67] See May 2011 "Third Declaration" of Phil Miller filed in *LSSi Data Corp vs. Comcast Phone, LLC*, Case No. 1:11-cv-1246, United States District Court For The Northern District of Georgia, retrieved through PACER.

[68] April 29, 2011 Second Declaration of Dennis G. Ainge, in *LSSi Data Corp vs. Comcast Phone, LLC*, Case No. 1:11-cv-1246, United States District Court For The Northern District of Georgia.

[69] Staff Opening Brief at 32, fn 104, citing Tien Testimony. When asked about the evils of data brokers, witness Tien pointed to the need "for people being able to control their information." *Id.* At no point did Comcast counsel challenge Mr. Tien's characterization of Targus/Neustar as a databroker.

took responsibility but which would not have happened but for its work with Neustar. The point where Targus/Neustar's roles as directory list licensing agent and data broker meet is in the use of Comcast data in a Neustar file called DLP, which consisted of Comcast data, data from at least one other large cable company, and a national consumer database sometimes referred to as Neustar's PCP or Pure Consumer Premium database.[70] Staff believed the Comcast customer data, including non-published numbers, were used in this way to corroborate Targus' consumer database(s).[71] These consumer databases were then sold to third parties, as a Targus/Neustar representative testified:

> [T]he types of companies that will license that [PCP] product are foundational data companies such as credit bureaus, people who are doing fraud prevention. Anybody who has a need for [that] sort of foundational household level consumer file in support of their business activities.[72]

Businesses that have "a need for that sort of foundational household level consumer file" are, in addition to credit bureaus and fraud prevention services identified in the Targus/Neustar manager's testimony, also debt collectors and telemarketers.[73]

---

[70] Staff Brief, at 32.

[71] *Id.* at 33-34. Although specific reference to the name of the Targus/Neustar database was largely avoided during the CPUC evidentiary hearings to protect alleged confidentiality interests, Neustar is much more expansive on its website. *See* http://www.neustar.biz/information/docs/pdfs/solutionsheets/pure-consumer-solution-sheet.pdf (last accessed May 25, 2016) ("Enhance Your Direct Marketing Files … Pure Consumer is built on Neustar's unique market-proven, consumer insights engine …Neustar raises the consumer data bar. We have proprietary partnerships with hundreds of data sources that report data numerous times daily. This means we also update our data several times each day. The result, you receive the most comprehensive, freshest consumer information … … Pure Consumer Premium delivers the maximum household coverage for direct marketing and base-file compilations").

[72] Staff Brief at 34, and fn. 108.

[73] *Id.* at fn. 109 and accompanying text.

Not only was the personal information of approximately 75,000 non-published customers likely used in the building of a national marketing database, and multiple variations of same sold to and used by credit bureaus, debt collectors, telemarketers, and others, but Targus/Neustar also sent Comcast's customer information back to Comcast for use on its Ecolistings website and possibly other uses, combined with information from other carriers apparently derived from that same national all-carrier customer database.[74]

Although the California investigation focused only on the fate of the non-published names, addresses, and telephone numbers, *the salient fact for purposes of the this NPRM is that broadband carriers may be sharing not just directory lists, but a exponentially larger data set of broadband data, with data marketers*.

The distribution system can be wide-ranging and complex. In the Comcast case, Targus' affiliate Localeze entered into a 2009 contract with kgb, a company which operated a nationwide directory assistance platform,[75] as well as an online "peoplefinder" website.[76] Whether kgb USA uses the Comcast listings in any other way is not something not even Comcast knows for sure, as there were no audit or oversight procedures in place.[77] Once the data was posted on the Comcast or kgb website, it could

[74] *Cf.* Staff Opening Brief at 38-39, and fn. 126.

[75] Kgb USA (the fuller legal name of the entity) was previously known as INFO NXX. Comcast has used kgb/INFO NXX to provide directory assistance to its customers since 2003. *See* Staff Brief at 37-38, and fn. 122.

[76] *Id.* at 38 and fn. 123, citing screenshots from www.kgbpeople.com (visited October 2014).

[77] *Id.* at 29-30.

go anywhere, as Comcast's Privacy Notice disclosed (continues to disclose) in the fine print:

> Once our subscribers' names, addresses, and telephone numbers appear in telephone directories or directory assistance, they may be sorted, packaged, repackaged and made available again in different formats by anyone.[78]

Whether this one-sentence disclosure adequately provides consumers with notice of the data marketing ecosystem into which they are consigning their personal information is doubtful, and a topic that is taken up below.

B. The Difficulty in Securing Adequate Disclosures and Consumer Choice Mechanisms.

The NPRM cites privacy notices and disclosures from a number of carriers, and asks whether proposed disclosure requirements will "ensure that BIAS customers receive sufficient information to give them confidence … [and] sufficient ability to decide whether and when to opt in to the sharing of data with third parties."[79] The NPRM and the attached proposed regulations contain much aspirational language – e.g., "be comprehensible and not misleading" – with which the California parties can hardly quibble, but which regulations become almost parodies of themselves when juxtaposed with the dense, slippery, and confusing language which carriers currently use to make their privacy disclosures.[80] Again, the Comcast case offers a concrete example, and

---

[78] *Id.* at 39, and fn. 128, citing Comcast Privacy Notice, at 6; *also available at* http://cdn.comcast.com/~/Media/Files/Legal/CustomerPrivacy/CustomerPrivacy.pdf?vs=3 (last visited May 21, 2016).

[79] NPRM, at ¶ 84; *see generally* ¶¶ 82-105.

[80] *See, e.g.*, NPRM Appendix A, proposed regulation 64.7001(a)(5).

again we caution that we have no reason to believe that Comcast is better or worse than other carriers in this regard (or other businesses like banks and online services). The single-spaced, fine-print, and highly-lawyered privacy notices that regularly arrive in consumers' mailboxes are – more often than not – simply consigned to the recycling bin.

The Comcast disclosure cited in the NPRM is of this type.[81] Aside from some formatting changes, the omission of reference to caller-ID blocking and the FTC's Do Not Call list, and the truncation of its description of non-published numbers, the current Privacy Notice appears largely identical to the notice/disclosure litigated in the CPUC Investigation.[82] When copied from the website into a Word document, the current Privacy Notice runs to 14 pages, and contains many legal terms of art incomprehensible to any layperson. It soothes with descriptions of the "limitations" on Comcast's data gathering and repeated references to how Comcast "protects" the consumer's individual data, but it is *entirely devoid of any disclosure (other than the one quoted above) that would alert the average consumer to the extensive distribution of the consumer's personal information described above,* much less to the sophisticated use of cookies and other tracking mechanisms that broadband providers use to harvest consumer data.[83]

//

[81] NPRM, at fn. 183.

[82] As quoted above. *See* http://cdn.comcast.com/~/Media/Files/Legal/CustomerPrivacy/CustomerPrivacy.pdf?vs=3 (last visited May 21, 2016)

[83] A further complication, from an enforcement perspective, is to trace what disclosures carriers made at any particular point in time. Apart from operations like archive.org, that make it their business to archive at least some of the Internet's exploding content, it is hard to track back to what a carrier disclosed and how the disclosure was presented at a given point in time.

(1) Information Asymmetry Generally.

As the Senate Committee on Commerce, Science and Transportation (Senate Commerce Committee herein) reported last year, "data brokers operate behind a veil of secrecy":

> Data brokers typically amass data without direct interaction with consumers, and a number of the queried brokers perpetuate this secrecy by contractually limiting customers from disclosing their data sources. Three of the largest companies – Acxiom, Experian, and Epsilon – to date have been similarly secretive with the Committee with respect to their practices, refusing to identify the specific sources of their data or the customers who purchase it.[84]

The obsession with secrecy in the data industry may explain the obfuscation and misdirection evident upon inspection of Comcast's Privacy Notice, and exacerbates a reality present in every agency enforcement case: the communication provider knows its business better than regulatory staff or the public ever will.

"Information asymmetry" exists not only between regulators and utilities generally, and staff and Comcast particularly, but also between Comcast and its customers. As the Senate Report put it:

> [D]ata brokers remain largely invisible to the consumers whose information populates their databases. Consumers have limited means of learning that these

[84] Senate Committee on Commerce, Science and Transportation, "A Review of the Data Broker Industry: Collection Use and Sale of Consumer Data for Marketing Purposes" (December 2013), at iii. available at http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=bd5dad8b-a9e8-4fe9-a2a7-b17f4798ee5a; *see also* Federal Trade Commission, "Data Brokers – a Call for Transparency and Accountability"(May 2014), available at http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf; and US General Accounting Office (GAO), "Information Resellers – Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace (September 2013), available at http://www.gao.gov/assets/660/658151.pdf.

> companies hold their data, and respondent companies provide consumers rights of access and control regarding their data that vary widely by companies. Several of the largest respondent companies have been similarly secretive with the Committee, refusing to identify specific sources of their data, and specific customers who purchase it. And provisions in company contracts with customers perpetuate this secrecy by placing restrictions on customer disclosures regarding data sources.[85]

While Comcast can obtain complete profiles of its customers, the customers have little or no idea what Comcast does with their data. This is particularly true of the non-published subscribers, who have an expectation of complete privacy that is at odds with the reality of what little privacy their $1.50/month actually purchases, even when the system works the way Comcast intended it to work.[86] In an attempt to remedy this problem, staff proposed a simple one-page/one-screen combined disclosure and opt-out of all information sharing (and opt-in to all available privacy products, including Caller ID blocking, CPNI protections, do not call lists, and non-published listings).[87]

Information asymmetry also becomes litigation strategy: the use of CPUC confidentiality rules to block public disclosure of key details, including of how customers' personal information is handled, as reflected in the redactions found in the public version of CPUC Staff's briefs; and the increasing misuse by carriers of the Electronic Communications Protection Act (ECPA) and CPNI rules to obstruct public oversight and prevent regulatory agencies from learning the victims of carrier negligence

[85] Senate Report, at 12-13.

[86] Customers uniformly reported to CPUC staff that they thought a non-published number meant that no one would see their number except Comcast. See evidence cited at Staff Opening Brief, p. 21, fn. 65.

[87] *Id.* at 121

and fraud.[88] The Commission should carefully craft its rules so that they will not be used to obstruct the very transparency they are intended to promote.

(2) Carriers' Privacy Disclosures Are Not Meant to be Read or Understood.

An comparison of Comcast's Privacy Notice with its marketing materials revealed something of a bait-and-switch tactic (and again, Comcast may not be an anomaly in this regard). Comcast's Welcome Kit stated that "Non-published directory Service ensures that Comcast will not make your phone number available in the phone book, an online directory or through Directory Assistance," while its Privacy Notice took that assurance away: "We take reasonable precautions to ensure that non-published and unlisted numbers are not included in our telephone directories or directory assistance services, but we cannot guarantee that errors will never occur."[89]

Comcast's chief witness on the customer interface introduced a third document, a customer agreement, which appears to bind the customer to the terms of the Privacy Notice that Comcast "cannot guarantee that errors will never occur."[90]

It is unlikely that a customer reads and digests any of this information. While the Welcome Kit with its "ensure" language is relatively large-font and reader-friendly, the Privacy Notice and customer agreement are written in a smaller font, and packed with legal terms and disclaimers. During her deposition Comcast's customer interface witness

[88] *See* Comcast Reply Brief, *infra*, at 47-48.

[89] Staff Opening Brief, *supra*, at 51-52. This language is also found in current Comcast Privacy Notice.

[90] *Id.*

was asked when and if a customer would receive the Privacy Notice and customer agreement, and her initial response was that she did not know.

> Q. And how does in your mind a customer manifest his or her agreement to those terms and conditions?
> A. I believe that they accept these terms at the installation or activation of service.
>
> Q. Do they have to – do they sign something that shows they
> A. I'm trying to think. I know that there's -- there may be a statement for instance on the installation work order that this is the acceptance of the terms. But I don't know all the legal ins and outs….
>
> Q. Is it your testimony … that the customer Comcast agreement for residential services is always attached to and provided with the privacy notice, if you know?
> A. I don't know.[91]

Comcast's witness confirmed in her prepared testimony that the Privacy Notice and customer agreement are provided "upon enrollment,"[92] and testified at her deposition that a customer would see the Welcome Kit (which includes the Privacy Notice and customer agreement) "at installation."[93] What that actually means is a little less clear:

> A. [T]he customer does accept the work order in some fashion, which because it's electronic now, they may be signing an electric device.
> Q. Right. Or clicking.
> A. But the welcome kit for a professional install. Meaning someone comes to the house. Is supposed to be handed to the customer.
> Q. Okay.
> A. And that would include those documents. The welcome kit itself, it should also include a privacy notice and the agreement in written form. And if they do not get a

[91] *Id.* at 52.

[92] *Id*.

[93] *Id.*

> professional installation, if they order a self installation, they're provided with these materials in that kit.[94]

From this, CPUC staff concluded that the customer was either given the Welcome Kit and included documents when the professional installer arrives, and asked to sign a work order accepting the terms and conditions of sale, or the customer who did a self-install was required to "click through" an acceptance of the terms and conditions prior to receiving the Welcome Kit and necessary equipment.[95] In either case, it seemed highly unlikely that a customer would have studied the Privacy Notice in any detail prior to signing the work order or clicking the online acceptance of terms. The Privacy Notice at issue in the CPUC Investigation did not itself have any place for a customer to initial, acknowledging they have read it (which would most likely have been a meaningless assertion in any event), and this is certainly the case with Comcast's current online Privacy Notice as cited in the NPRM.

(3) Even when Read, the Language of the Privacy Notice Is Confusing and Impossible to Understand.

Comcast's Privacy Notice -- as cited by the FCC and litigated before the CPUC -- covers a number of different topics. The current Privacy Notice focuses primarily on Customer Proprietary Network Information (CPNI), Personally Identifiable Information (PII).

//

[94] *Id.*, at 52-53.

[95] *Id* at 53.

a. Customer Proprietary Network Information (CPNI)

The current Comcast Privacy Notice cited in the NPRM more or less tracks the statute in defining CPNI as "phone information about the quantity, technical configuration, type, destination, location, and amount of your use of the phone services, and information contained on your telephone bill."[96] Later it adds that this could include "calling patterns." The Privacy Notice might have translated this into plain English: information about who you call, when you call them, and how long you talk to them.

Nor does the current online Privacy Notice instruct a customer how she can opt out of disclosure of such "calling patterns," (or explain what other protections are available, e.g., non-published numbers). The Privacy Notice states:

> We explain below under "HOW DO I GIVE OR WITHHOLD MY APPROVAL FOR COMCAST TO USE CPNI TO MARKET ADDITIONAL PRODUCTS AND SERVICES TO ME" how you can approve our use of CPNI or withdraw approval in the event Comcast decides to use CPNI for marketing purposes.

Only there is no there there (or "below" below). The customer reads on, in vain, to understand exactly what steps she must take to "withhold" her approval for Comcast's use of CPNI (or even what that means in practical terms). The section labeled "How do I give or withhold my approval for Comcast to use CPNI to market additional products and services to me?" holds out the hope of some clear advice on how to opt out of data sharing, but instead the consumer reads this:

> Various direct and indirect subsidiaries and affiliates of Comcast Cable Communications, LLC offer many

[96] *Compare* 47 USC §222(c).

> communications-related and non-communications related services, such as high-speed Internet and home security services. From time to time we may like to use the CPNI information we have on file to provide you with information about our communications-related products and services or special promotions. Our use of CPNI may also enhance our ability to offer products and services tailored to your specific needs. In addition, Comcast also offers various other services that are not related to the services to which you subscribe. Under the CPNI rules, some of those services, such as Comcast cable video services, are considered to be non-communications related products and services. Therefore, you may be asked during a telephone call with one of our representatives for your oral consent to Comcast's use of your CPNI for the purpose of providing you with an offer for communications related or non-communications related products and services. If you provide your oral consent for Comcast to do so, Comcast may use your CPNI only for the duration of that telephone call in order to offer you additional services.
>
> If you deny or restrict your approval for us to use your CPNI, you will suffer no effect, now or in the future, on how we provide any services to which you subscribe.

Neither this section, nor any other part of the Privacy Notice, explain what a consumer most wants to know: exactly what the customer has to do to block *all* sharing of CPNI, PII, and all other personal data except what is absolutely necessary to provide the service.[97]

b. Personally Identifiable Information

The Comcast referenced in the NPRM defines Personally Identifiable Information (PII) as information needed "in order to provide reliable, high quality service to you, we keep regular business records containing information about you that may constitute

[97] *Compare* Schneier, *Data Goliath, supra,* at 203 ("make data collection and privacy salient").

personally identifiable information." The translation here is "billing" and related information. Comcast continues, "These account records include some, but typically not all, of the following information:

- your name;
- service address;
- billing address;
- e-mail address;
- telephone number;
- driver's license number;
- social security number;
- bank account number; and
- credit card number."

Much further down in the current online notice, we find a long litany of all the uses to which Comcast puts personally identifying information, none of which hint at the trade in account listings described above:

- billing and invoicing;
- administration;
- surveys;
- collection of fees and charges;
- marketing;
- service delivery and customization;
- maintenance and operations;
- technical support;
- hardware and software upgrades; …
- fraud prevention ...
- install, configure, operate, provide, support, and maintain our cable service and other services;
- confirm you are receiving the level(s) of service requested and are properly billed;
- identify you when changes are made to your account or services;
- make you aware of new content, products, or services that may be of interest to you;
- understand the use of, and identify improvements to, our services;
- detect unauthorized reception, use, or abuse of our services;
- determine whether there are violations of any applicable policies and terms of service;
- manage the network supporting our services;

- configure and update cable service and other service-related devices and software; and
- comply with law[;]
- send and receive e-mail, video mail, and instant messages;
- transfer and share files;
- make files accessible;
- visit websites;
- place or receive calls;
- leave and receive voice mail messages;
- use the applicable communications center or voice center;
- establish custom settings or preferences;
- communicate with us for support; or
- otherwise use the services and their features.

Nowhere do we get the kind of disclosure that would really matter to consumers (yes, we share your data with nationwide data marketing companies), much less the disclosure envisioned by California's "Shine the Light" law (which is, however, provided only "on request"):

> * the names and addresses of all the third parties that received personal information from the business in the preceding calendar year; and
>
> * if the nature of the third parties' business cannot be reasonably determined by the third parties' name, examples of the products or services marketed by the third party.[98]

Two-thirds of the way into the current Privacy Notice, buried in the fifth paragraph of a section about "activity data" (also a topic fraught with consumer exposure), is perhaps the essential disclosure, one which echoes the iterative exchanges of databases between Comcast and Targus/Neustar found in the CPUC investigation: "We may also combine personally identifiable information, which we collect as described in this notice as part of our regular business records, with personally identifiable information obtained

[98] NPRM at ¶ 85, citing Cal. Civ. Code § 1798.83.

from third parties for the purpose of creating an enhanced database or business records." This hardly a clear and conspicuous disclosure More importantly, *nowhere* is the consumer given the opportunity to opt out of this data-base compilation, or other sharing of personally identifiable data with third parties.

(4) The Lack of Disclosure re Non-Published Numbers, Do Not Call Lists, & Caller ID Blocking, and the Difficulty Finding a Privacy Notice on Comcast's Website.

The Privacy Notice cited in the NPRM has eliminated any detailed discussion of privacy services like Non-Published Numbers, the FTC's Do Not Call list, or caller ID Blocking from the form of notice litigated before the CPUC.[99]

And it remains difficult to find. In the CPUC investigation, staff documented just how difficult it was to find the Privacy Notice on Comcast's website. The link to the Privacy Notice was not located on Comcast's home page. Instead one had to navigate four levels down from the home page to locate the link to the Privacy Notice. The only way staff was able to locate the Privacy Notice on Comcast's website was to enter the words "Comcast" and "CPNI" into the Google search engine, which provided a link that took staff to a Privacy Notice four levels below the Comcast homepage.[100]

In all of this, however, the salient point is that Comcast did not then, and does not now, disclose in any meaningful way that it was and likely still is – directly or indirectly -- sending personal information to data marketers and brokers.

---

[99] *Compare* discussion in Staff Opening Brief, at 55-57.

[100] *Id.* at 58, citing http://www.comcast.com. The provision of the Settlement Agreement that a Simplified Disclosure be available "in a readily accessible location" was designed to address this, but is only in effect for three years. *Compare* Settlement Agreement, *supra*, at Section 3(b).

C. The Challenge of Creating Effective Disclosure and Consumer Choice Mechanisms.

Disclosures to customers in this complex area should be as understandable as possible to the majority of a carrier's subscribers, perhaps using standard measures of readability like the Flesch-Kincade Grade Level Index.[101]

But even if carriers could be required to provide disclosures understandable by their customers, the greater problem is still outstanding: creating *effective* choice mechanisms. Although the Comcast Settlement Agreement calls for a Simplified Disclosure form in a "readily accessible location" on the carrier's website,[102] Commission staff had originally suggested something more, that Comcast provide such a simplified disclosure *and* "allow consumers the option to opt into all of these protections, and to opt out of any and all data sharing to the full extent provided by law, preferably with one click or check mark or postcard." [103]

Alternatively, the FCC could require something along the lines of a "Schumer Box,"[104] not unlike the Simplified Disclosure called for in the CPUC-Comcast Settlement

---

[101] The Flesch-Kincaid Grade Level index is one way to measure how difficult a text is to understand. The formula considers the average number of words per sentence and the average number of syllables per word within a given passage. The results are then converted into a score that roughly equates with a grade level in the United States. See www.readabilityformulas.com/flesch-grade-level-readability-formula.php.

[102] Settlement Agreement, Section 3, and Exhibit C (mock-up of the disclosure required to be provided to consumers and posted in a readily accessible location on Comcast's website). The Settlement Agreement is available at http://docs.cpuc.ca.gov/PublishedDocs/Published/G000/M154/K464/154464133.pdf.

[103] Opening Brief, at 121.

[104] The Schumer Box was designed to make credit card interest disclosures easily understandable. It is encoded in "Regulation Z", and found at 47 CFR 226.5a(a)-(g), available at https://www.law.cornell.edu/cfr/text/12/226.5a; *see also* report of Consumer Compliance Outlook, at https://consumercomplianceoutlook.org/2009/first-quarter/q1_03/; https://en.wikipedia.org/wiki/Schumer_box. Authorized by Congress in 1988, and amended in 2009,

Agreement, *but with opt-in and opt-out choice mechanisms* – either an online click or a hard-copy check the box –*all in the same document.* The sophistication of carrier (or carrier-partner or carrier-affiliate) data mining today is so great that carriers should be required to go to extra lengths to make their disclosures and choice mechanisms as clear as possible. A standardized form, as the Commission suggests, would help accomplish this.[105]

Carriers should also be required (if they are not already) to maintain superseded privacy notices for a period of ten years, and provide them on request. Finally, especially important in a multi-ethnic state like California, is in-language disclosures, particularly when the carrier advertises in-language.

D. In a Digital World, Carriers Must Be Vigilant to Protect Consumers' Personal Information, by Prevention and Early Detection of Data Breaches.

The *NPRM* presents a "data security framework," consisting of strategies to help telecommunications carriers prevent, detect, and remediate data breaches, including but not limited to: regular risk management assessments; training in security procedures for employees, contractors and affiliates that handle customer information; designation of a senior management official responsible for implementing data security; establish responsibility for use of the customer PI by third parties, and accountability for its

---

there are still questions whether the "honesty box" is adequate to the task of providing consumers with sufficient information to make informed marketplace decisions.

[105] Id. at ¶ 90 (whether "notices should be standardized to allow better comprehension and comparison").

misuse; and restricting access to sensitive data.[106] The structural weaknesses uncovered in the *Comcast Investigation* demonstrate the wisdom of these measures.

(1) Prevent: Risk Assessments, Terms in Contracts with Third Parties, Training.

Risk assessment must be directed toward the types of information collected, and the real-world ecosystem in which that information is collected, stored, used, and provided to third parties. In the current industry environment, where everything from billing to directory assistance to customer service may be contracted out to third parties, carrier risk assessment necessarily means monitoring how third parties' use the data, while for the regulator it means holding the principal carrier liable for any breaches that occur.

Like many telecommunications carriers, Comcast used a number of third parties to help it manage its data. That Comcast would send *non-published* account information beyond its own walls, even if that did not violate the implicit understanding of consumers that non-published meant private, was in any event a reckless act that may have been driven by a desire to play ball with the data marketers.[107] It clearly increased the vulnerability of that data to misuse.[108] Expert witness Tien expressed succinctly the peril to which this exposed Comcast's non-published customers:

> My concern here is that because Targus is in a business of data aggregation and data dissemination, then when – that it can magnify the harm or the exposure of personal information

[106] *Id.* at ¶¶ 175, 167-232.

[107] *See* Staff's Opening Brief, *supra*, at 61-64.

[108] Staff Opening Brief at 60, and footnote 200.

> such as the non-published numbers if there is an error or, you know, that leads to them receiving information that they should not – that should not have been given them in the first place.[109]

Every further third-party contractor through which the data travels increases the peril. Here, the directory listings went through a number of hands in addition to Targus/Neustar, including kgb, a national directory assistance firm, and LSSi, a well-known data broker also serving as a directory listing distributor (although Comcast claimed the non-published numbers did not go to LSSi).

Also important are the sheer number of tasks that were outsourced to some extent or other: billing; customer service; storage of customer service records. Part of the settlement with Comcast required that vendors to which the directory listings go are now required to acknowledge the confidentiality of the directory listings and not use them for any other purpose.[110]

In this environment, regular training of carrier employees and contractors, emphasizing customer privacy interests, is also a key component of a breach prevention program.

(2) **Detect: the Commission Should Consider Mandating the Monitoring of Trouble Tickets** and Other Early Warning Signs.

The fact that it took a major carrier like Comcast almost two-and-a-half years to detect a wide-spread privacy breach indicates that this was a low-priority for the carrier.

[109] *Id.* at 60.

[110] Settlement Agreement, *supra*, at section 2.

Federal standards, that include (for example) the monitoring of trouble tickets and other customer input, could provide a checklist and incentive for challenged carriers.

The record clearly establishes that Comcast had multiple opportunities to discover the breach in 2010, 2011, and early 2012. These include approximately 75 California Trouble Tickets from 2010 that Comcast admitted were related to the "Process Error," an estimated 770 total California customers who contacted Comcast about related non-published number issues before discovery of the breach, at least six Comcast internal emails warning of problems with non-published numbers, *and* a February 2012 KCBS Sacramento television story on publication of one irate customer's non-published number – ten months before the breach was discovered.[111] This does not include customer narratives posted on Internet complaint sites, including Comcast's own customer complaint website, as well as internal suggestions that perhaps a "root cause" analysis would help detect the cause of rising "escalations."[112]

Regular and conscientious monitoring of customer trouble tickets, and performance of a root cause analysis when problems present themselves repeatedly, could have nipped this breach in the bud, certainly short of the two-and-one-half year mark.

E. The Commission Must Rule that All Information About a Customer Collected by a Carrier Is "Proprietary" to the Customer, and Must Deny the CTIA Petition to Reduce these Protections for Low-Income Consumers.

The Commission asserts that "today's broadband providers do not publish directories of customer information," that "mobile providers have never published

[111] *See* Staff's Opening Brief, at 44-49.

[112] *See, e.g., id*, at 45, 49.

subscriber list information," and that "in the fixed context, customers have long had the option to request such customer information not be disclosed," which the Commission finds "inherently recognize[s] the personal nature of such information."[113] On that basis, the FCC proposes that "there is no subscriber list information in the broadband context." Although this statement may not be entirely correct (most broadband carriers, like Comcast, have telephone affiliates), and although the Commission may underestimate the continuing consumer vulnerabilities created by the use, sale, and/or sharing of consumers' (directory) listing information, it comes to the right conclusion: "BIAS customers' names, postal addresses and telephone numbers should be treated as PII.[114]

This conclusion has obvious ramifications for the CTIA petition for Partial Reconsideration in the *Lifeline* proceeding, which seeks to "clarify" – at least in the Lifeline context, where low-income consumer data is at issue – that "proprietary" information in section 222 does not include anything except the technical CPNI listed in that section.[115] It is inconceivable to the California Parties that a customer's essential identifying information – name, address, telephone number, which are not specifically referenced in, or are specifically excluded from, the CPNI definition – would not be protected by the primary privacy protection statute in the Communications Act.

[113] NPRM, at ¶ 64.

[114] *Id.*

[115] CTIA Petition for Partial Reconsideration, *In re Lifeline Reform and Modernization,* WC Docket 11-42 et al. (Aug. 13, 2015). Section 222 of Title 47 defines CPNI as "quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service."

Even if there is "no subscriber list information in the broadband context," there is subscriber list information associated with VoIP numbers and listings,[116] and in a more practical sense, there is not much if any difference between telephone subscriber listing and broadband billing information – except that the FCC decisions defining a directory listings marketplace have given carriers cover to trade in this data. Thus, it is particularly important that the Commission protect Subscriber List or Directory Listing information, given that the clear value of this data.

Precisely this directory listing information, or billing information masquerading as directory listing information, falls within a loophole (and potential Pandora's Box) in the privacy protections of Section 222:

> (e) Subscriber list information.
> Notwithstanding subsections (b), (c), and (d) of this section [carrier information and CPNI protections], a telecommunications carrier that provides telephone exchange service *shall provide subscriber list information* gathered in its capacity as a provider of such service on a timely and unbundled basis, under nondiscriminatory and reasonable rates, terms, and conditions, to any person upon request for the purpose of publishing directories in any format.

This section, in conjunction with Section 251(b)(3), has created a market in directory listings, and spawned a significant amount of litigation between telecommunications carriers and data brokers, trading allegations of discrimination,

[116] Comcast had both telecommunications and IP affiliates in California; even though the IP affiliate was the nominal vendor of retail services to the end-user, all numbering and directory listing issues were handled by the telecommunications affiliate (and CPCN holder). See Order Instituting Investigation 13-10-003, *supra*, at 4-5.

contract breach, and improper conduct.[117] In Comcast's case, *LSSi* demanded that Comcast continue to deliver the directory listing information even after Comcast determined LSSi was a bad actor and attempted to terminate its directory listing contract with LSSi.[118]

In its briefs, Comcast essentially argued that the 1996 Act, and particularly Section 222(e), required it to provide the directory listings (including non-published numbers[119]) to any third party who asked, because the "promoted competition in the telecommunications market by preventing providers from excluding their competitors' listings from phone books, online directories, and directory assistance databases."[120] This is both true and misleading at the same time. The sharing itself was not mandatory, but once the carrier made the decision to license to third parties, the carrier was barred from discriminating among "qualified" third parties – directory assistance providers and directory publishers, thus vastly expanding the reach of any possible breach of non-published numbers, and illustrating the wide network of companies in the information marketplace with potential access to subscribers' personal data.[121] In Comcast's case, the

[117] *LSSi v. Comcast*, 696 F3d 1114, 1119 (11th Circuit, 2012), *on remand LSSi v. Comcast*, 2013 U.S. Dist. LEXIS 188580 (D. Ga., March 4, 2013); *see also LSSi v. Time Warner Cable,* 892 F. Supp. 2d 489 1(SDNY 2012).

[118] Comcast Reply Brief, *infra,* at 41-44.

[119] Staff Opening Brief, at 59-63, reciting Comcast's unlikely rationale for sending the non-published numbers to Targus/Neustar along with the numbers, so they could be "found" by directory assistance operators, who could report to the customer that the number existed as an unlisted phone number.

[120] Comcast Opening Brief, *supra,* at 8, and fn. 22, citing FCC's Third Report and Order *In re Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information,* et al., 14 FCC Rcd. 15550 ¶ 86 (1999).

[121] The FCC promulgated a rule requiring a carrier like Comcast to provide non-discriminatory access to its subscriber lists *if* it provides any access at all. None of this blocks the ability of a carrier to audit what

data went first to Targus/Neustar, and then through one of its affiliates ("Localeze") to a directory assistance provider by the name of "kgb," which itself ran an online directory service, and also to another known data broker LSSi

Nor was Comcast's argument that "222(e) made me do it" particularly credible. Comcast first claimed that it was required to provide Directory Listing information to data marketers Targus/Neustar and LSSi under 222(e),[122] and then reversed field and claimed that LSSi was "neither a LEC nor a directory publisher" *per se*, and therefore "LSSi was not entitled to the same rates as kgb."[123] The evidence suggested that the reality was a free-for-all marketplace, in which telecommunications providers, directory listing providers, directory listing distribution agents, and data marketers all vied to control the directory listing information at the most advantageous terms. It further suggests that the legally mandated exchange of subscriber information for telephone

---

downstream uses of its carrier lists the publisher or DA provider is actually making FCC Third Report and Order, *supra; see also* Order on Reconsideration, *In re Implementation of the Telecommunications Act of 1996: Telecommunications Carriers Use of CPNI and other Customer Information,* 19 FCCR 18439 (2004) at ¶ 18 carriers may bring a civil action for breach of contract if directory publishers misuse subscriber list information. The prospect of such suits should help deter entities from misusing subscriber list information obtained pursuant to section 222(e).

[122] Comcast, Opening Brief, at 7-8 (1996 Act "require[ed] LECS to share their directory listing information with other LECs and directory publishers"), and fn. 21, citing Section 222(e); *see also* April 29, 2011 Declaration of Phil Miller in *LSSi v. Comcast*, US Dist. Court for the N.D. of Georgia, Case No. Case No. 1:11-cv-1246, at ¶¶ 5-6 (claiming that LSSi could license the DLI/SLI at the "same rates. terms, and conditions" as Comcast applies to itself or any directory publisher).

[123] Comcast Reply Brief, at 44 (available at http://docs.cpuc.ca.gov/PublishedDocs/Efile/G000/M143/K958/143958564.PDF). Despite thus admitting in the CPUC proceeding that it was rate-discriminating against LSSi, Comcast apparently led the District Court and 11th Circuit to believe that it was not. *LSSi v. Comcast,* 696 F3d 1114, 1123 (11th Circuit, Sept. 26, 2012) (LSSi unlikely to prevail on rate discrimination claim). The District Court later referred the matter to the FCC, where it apparently became docket 14-211, and was dismissed by stipulation in October of last year.

directories may have been, and may be still, an excuse for direct or indirect transactions between network carriers and data aggregators, marketers and brokers.

The extent of the trade in personally identying/indentifiable information in the telephone world should put the FCC on alert to the vastly increased dangers in a broadband world.

In light of Comcast's arguments and marketplace reality, it is important that the FCC adopt its proposed rule that customer proprietary information in 222(a) goes beyond the CPNI protected in 222(c) and defined in 222(h)(1) (which excludes "subscriber list information" from the CPNI protections), and includes "personally identifying information" whether or not it is proprietary *network* information, especially where the customer opts to keep such information as name, address and telephone number confidential. There can be no argument that a subscriber's name, address, and telephone number – *when that customer has paid $1.50/month for an unlisted/non-published number* – are proprietary to the subscriber. To rule, as CTIA petitions, would be to empty the word "proprietary" of any meaning. Nor should carriers be allowed to abandon the non-published option.

It is therefore important that the FCC reiterate that the "subscriber list" exception to CPNI applies narrowly, relates only to listing information exchanged between those actually in the business of publishing directories and actually used for that purpose, and in no event includes listings which the customer has requested remain non-published.

//

F. Role for State Enforcement

The FCC proposes not to preempt state laws and efforts to enforce them so long as such laws and enforcement are "consistent" with the Commission's approach to Section 222.[124] Commenting Parties believe that the *Comcast* case speaks for itself of the value of state law enforcement. The CPUC and Intervenors were closer to witnesses, closer to local media where evidence of the breach surfaced, and better able to apply narrowly tailored state law. Despite the FCC's impressive enforcement record of late, neither federal nor state agencies have sufficient resources to fully protect consumers, and it is important that "cooperative federalism" be maintained in this vital area.

V. CONCLUSION

Located in the San Francisco Bay Area, a short freeway ride from Silicon Valley, the Commenting Parties have had a ringside seat for the creation of the Apple computer, the founding of the first online social spaces (e.g., the Whole Earth 'Lectronic Link),[125] and the invention of Google by two guys in a dorm, in the seventies, eighties, and nineties, respectively. We understand how digital and Internet-related technologies are changing lives at an exponentially accelerating pace, bestowing the benefits of social networking and an information cornucopia, which benefits however have a dark shadow (digital surveillance and the loss of autonomy over personal data). As much as has been written about the Twitter and Facebook revolutions in the Arab World, and "about the democratizing power of the Internet," we also remember that "in the hands of an

[124] NPRM at ¶¶ 276-277.

[125] *See* www.well.com.

authoritarian regime [the Internet] can become a tool of repression."[126] More to the point of the *Broadband Privacy NPRM*, in the hands of data marketers (or the carriers themselves) personal information has become a commodity, and broadband telecommunications carriers have become primary procurers of this data. This in turn creates a conflict of interest for the network operator, and reduces consumers' trust in the integrity of the communications network. The Commission needs to separate the communications transport and customer data markets, and ensure that consumers have clear choices in each.

Date: May 27, 2016

Respectfully submitted,

Paul Goodman
Greenlining Institute

Tracy Rosenberg
Media Alliance

[126] *See, e.g.*, Morosov, "The Dark Side of internet for Egyptian and Tunisian Protesters," *The Daily Globe & Mail* (Jan 28, 2011), available at http://www.theglobeandmail.com/news/world/the-dark-side-of-internet-for-egyptian-and-tunisian-protesters/article563944/.